The final publication is available at Springer

https://doi.org/10.1007/978-3-319-66284-8_24

Safety and Security Co-Engineering and Argumentation Framework

H. Martin[1], R. Bramberger[1], C. Schmittner[2], Z. Ma[2], T. Gruber[2], A. Ruiz[3], G. Macher[4]

[1]VIRTUAL VEHICLE Research Center - Graz, Austria
{helmut.martin, robert.bramberger}@v2c2.at
[2]Austrian Institute of Technology - Vienna, Austria
{christoph.schmittner,zhendong.ma,thomas.gruber}@ait.ac.at
[3]TECNALIA / ICT Division - Derio, Spain
alejandra.ruiz@tecnalia.com
[4]AVL List GmbH - Graz, Austria
georg.macher@avl.com

Abstract. Automotive systems become increasingly complex due to their functional range and data exchange with the outside world. Until now, functional safety of such safety-critical electrical/electronic systems has been covered successfully. However, the data exchange requires interconnection across trusted boundaries of the vehicle. This leads to security issues like hacking and malicious attacks against interfaces, which could bring up new types of safety issues. Before mass-production of automotive systems, evidences and arguments are required regarding two aspects. Product engineering has been done compliant to specific standards and supports arguments that the system is free of unreasonable safety and security risks.
This paper shows a safety and security co-engineering framework, which covers standard compliant process derivation and management, and supports product specific safety and security co-analysis. Furthermore, we investigate process- and product-related argumentation and apply the approach to an automotive use case regarding safety and security.

Keywords: Safety and security co-engineering • process- and product-based argumentation • process and argumentation patterns • automotive domain • ISO 26262 • SAE J3061

1 Introduction

The market and the society are requesting safe vehicles. Upcoming vehicle functions require external sensor data and communication across vehicle boundaries. Furthermore, software updates with new vehicle features can increase road safety, but these topics introduce the additional challenge on cybersecurity. Security issues are starting to be in the front line in the automotive business because more and more problems at the market occurred and have been published by various media. In 2015 the Jeep Cherokee become unfortunately famous for being hacked remotely [1]. Late-

ly vulnerabilities in Tesla [2] have also become real. In both cases core safety-critical elements such as the brakes became vulnerable. The main lessons learned with these experiments are that vulnerabilities are hidden in the inner design of the system. Security has to be considered at early stages of the concept design [3].

The industry and standardization committees are moving forward a collaborative approach between safety and security disciplines. Currently, automotive safety and security disciplines are not similarly mature - security is less mature than safety [4]: While the SAE guidebook regarding automotive cybersecurity is available in the first edition, for the established automotive functional safety standard ISO 26262 [5] the preparation of edition 2 is ongoing. Both documents note interaction points of functional safety and cybersecurity[1], but only in an informative way. The standards focus on guidance to solve the challenges in the specific safety and security lifecycle. One of the challenges identified in the ISO 26262 standard is the need of a safety case which provides argumentation in a clear and compressive way that a system achieves a reasonable level of functional safety to operate in a given context. While functional safety refers to safety against failures in electrical/electronic (E/E) components, in the future there has to be argumentation where not only safety but also security and probably other dependability aspects are covered.

The paper at hand deals with a concept that covers standard compliant process- and product-based argumentation in context of safety and security. Just by following the standards procedures, your system is not guaranteed to be free of risks. Standards are considered a compilation of best practices which describe industry-wide accepted concepts, methods and processes. The paper is structured as follows: Section 2 describes the state of the art and previous approaches for this problem. Section 3 presents the safety and security co-engineering framework proposed by the authors. Section 4 demonstrates how the approach depicted in is put into practice by using specific tools. Section 5 provides conclusions and an outlook on further work.

2 Background and Related Work

ISO 26262 is the automotive functional safety standard, describing a safety lifecycle for the development of safety-related automotive systems (targeting passenger cars and minivans). The first edition was published in 2011 and is currently in a revision phase. A new informative annex will define potential interaction and communication channels between functional safety and cybersecurity. The same concept of safety and cybersecurity interaction points is presented in SAE J3061 [6]. The security lifecycle specified in SAE J3061 proposes communication paths between safety and security engineering. Fig. 1 provides an exemplary overview of the interaction between safety and security engineering during the concept phase. The lifecycles itself are clearly described in the standards, but the interaction and cooperation is currently based on informative annexes which suggest approaches and potential coop-

[1] The term “safety” refers functional safety according to ISO 26262, and “security” refers to cybersecurity according to SAE J3061.

eration topics. Based on SAE J3061 a joint working group between ISO and SAE was started with the goal of developing an SAE/ISO "Standard for Automotive Cybersecurity". For safety and security co-analysis in different lifecycle phases multiple methods have been developed, e.g. STAMP (Systems-Theoretic Accident Model and Processes) [7] a theoretic model for safety, SAHARA (Security-Aware HARA) [8], an extension of the HARA method (Hazard And Risk Analysis) or FMVEA (Failure Modes, Vulnerabilities and Effects Analysis) [9], a combination of threat modeling and failure modes and effects analysis. But methods like these need to be embedded in a larger lifecycle framework. There is a need to define the open area between the standards.

Fig. 1. Comparison of safety- and security engineering

For safety and security it is required to provide evidence and argumentation to show that the system development was done compliant to relevant standards and that the system satisfies safety and cybersecurity goals. The final documentation has to be provided by the safety case and the cybersecurity case.

ISO 26262 mentions the possibility to use a graphical notation, **Goal Structuring Notation (GSN)** to create the safety case. GSN's initial intention was to support safety case management [10]. Ray and Cleaveland proposed to apply GSN for constructing security assurance cases of medical cyber-physical systems [11]. The graphic structure of the security assurance case starts with a top-level security claim node accompanied by context information node and then breaks into layers of sub claim nodes that argue over different stages and aspects of the development lifecycle. Each sub claim is supported by a set of evidence nodes that explain the validity of the claim. Basically, GSN for assurance case is a graphic way to organize narrative information of claim, context, strategy, argument and evidence according to the GSN convention.

Patterns are a suitable way to support argumentation that safety and security related requirements are fulfilled. They assist in reusing best practices systematically [16]. Menon et al. [12] demonstrate how patterns are used to provide argumentation structures for software safety arguments. The authors define the structure consisting of GSN elements and its applicability. Patterns are usable on all development levels. Preschern et al. [13] examine the relationship between security and functional safety. The authors present an approach to categorize threats related to the impact to safety-critical functions.

3 Safety and Security Co-Engineering Framework

Fig. 3 shows the main steps of the proposed methodology which considers all process steps necessary in an automotive safety and security related development project:

Regulations and Standards (I) and Process Development (II). In a first step we have to identify all relevant regulations and standards. In our automotive use case we have to deal with ISO 26262 regarding road vehicles functional safety and SAE J3061. It is challenging to match these two topics because they are influencing each other. Process developers have to consider that elaborated process steps are not only in parallel but also highly interactive, especially when we are focused on functional safety and cybersecurity. In addition, processes have to incorporate special analysis methods like STAMP which handles safety and security aspects in one common analysis methodology. Integrated processes which are basis for co-engineering unite safety with security activities. They lead to integrated requirements, work products and argumentation.

Process Management (III). The core of the framework is the distinction between functional safety and security related process and product requirements and the identification of interactions. Process requirements describe activities and steps which are demanded by standards, while product requirements are requirements from the system in development. In order to manage the processes and support the processes execution, appropriate tools are useful, which assist developers with requirement and work product management. Work products are process outcomes representing different types of evidence. Evidence shows capability and maturity of the development process, compliance to the underlying standards and safety as well as security of the developed products. In addition, evidence is used to support arguments which are related to requirements.

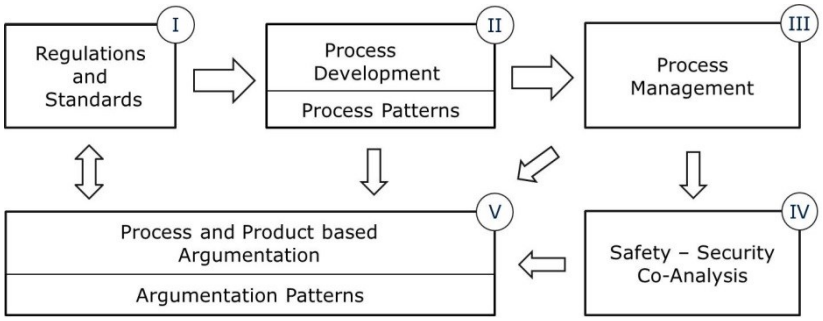

Fig. 2. Safety and security co-engineering framework

Safety and Security Co-Analysis (IV). The intention of the proposed framework is to integrate functional safety and security. For that reason we have to deal with special analysis methods like STAMP (see section 3.2) which handles safety and security aspects in one common analysis methodology.

Process- and Product-based Argumentation (V). Consequently the argumentation demonstrates that the item under consideration contains no unreasonable risk and

consolidates functional safety and security. To visualize these relationships between requirements and work products we use GSN. A more detailed description of the argumentation approach can be found in [16],[17].

To recapitulate we consider a loop (depicted in Fig. 5) in which every activity is supported by a tool. We start with regulations, create processes which are modelled, instantiated and executed. The output besides the product is evidence which is used to argue that activities for the development of a specific product have been performed and are compliant to the regulations. Once an integrated process has been defined various disciplines, like safety and security, have to coordinate their actions. In this case project managers have exact directives if developers from different disciplines resist doing cooperative work.

3.1 Process Management

The requirements-driven workflow during process management starts with capturing requirements derived from the system artefacts, from standards, and possibly other, e.g. domain specific sources. The goal is a valid combined safety and security case, which requires evidences for the arguments it is composed of. The next step in the process is the definition of the necessary assurance activities, for which appropriate tools and methods are assigned. Finally, the assurance activities are processed – as far as possible automatically by a workflow engine. Successful assurance activities yield the necessary evidences. In case of negative results the faulty system element needs to be amended and then the assurance activity needs to be re-processed. When all assurance activities have been processed successfully the combined safety and security case is complete and valid.

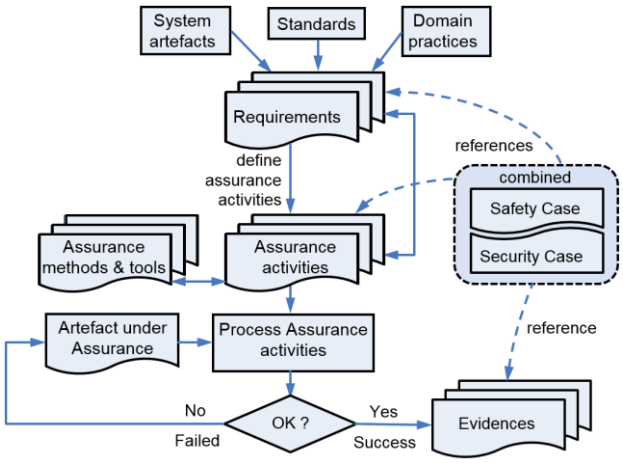

Fig. 3. Workflow model supporting compositional safety and security case

3.2 Safety and Security Co-Analysis

Integrated development processes have to deal with requirements concerning functional safety and security. They affect not only safety related methods (e.g. HARA), they also demand methods for joint safety and security analysis (e.g. STAMP, STPA-Sec, FMVEA).

STAMP proposes to model systems as hierarchical structures. Higher level controllers in the hierarchy control the processes at lower levels via actors, while the lower levels send feedback to the higher levels via sensors. It proposes that it is difficult to identify root causes for accidents in modern complex system. Therefore, safety accidents should be viewed as a result of a lack of control, instead of a chain or sequence of events such as in the Swiss cheese model. Based on the STAMP (Systems-Theoretic Accident Model and Processes) viewpoint System-theoretic Process Analysis (STPA) is a novel analysis approach based on a control theory based system consideration. System-theoretic Process Analysis for Security (STPA-Sec) [18] extends the safety-focused method to cover security. STPA-Sec consists of following steps:

Step 1. System description (scope, control model, accidents and hazards).

Step 2. Identification of unsafe control actions (using control actions from Step 1 and guidewords to identify unsafe control actions in all system states and environmental conditions). Control action not given, given incorrectly, wrong timing or order, stopped to soon or applied to long.

Step3. Identification of scenarios which can cause unsafe control actions: identify, based on control loop, scenarios how unsafe control action can be caused.

Step 4.Design controls and countermeasures based on scenarios.

In STPA-Sec, each control action is analyzed under different possible conditions and guide words to identify loss scenarios. A loss is a situation of insufficient or missing controls or safety constraints.

3.3 Patterns for Process and Argumentation

Patterns are a concept which spreads out in various development areas. We are using patterns to provide process and argumentation frameworks, which represents most of the recurring steps. The intention is to spend time once and reuse the elaborated patterns many times. Especially the integration of activities related to functional safety and security is a challenging work. We have created patterns that provide argumentation- and process- templates. Process patterns simplify creating development processes because they already bring together functional safety and security activities.

Argumentation patterns are corresponding to the process and exhibit the line of argumentation using the created work products. They include argumentation concerning trade-offs between functional safety and security. Both types of patterns have to be instantiated for the regarding project. Instantiation for example means to select project specific methods like STPA-Sec. In parallel the corresponding line of argumentation has to be selected. The purpose of creating patterns within the framework is to simpli-

fy process development and the elaboration of evidence and adequate fitting arguments to support the claims, which are related to requirements.

4 Application to the Use Case

The automotive hybrid powertrain board net use-case provides the basis for the analysis of safety and security aspects based on state-of-the-art material[2]. An integral part of the hybrid powertrain system is the high voltage (HV) battery system, which consists of the battery management system (BMS), the battery satellite modules (grouping battery cells in modules and communicating via dedicated bus), and a fan control for cooling of the battery cells. The BMS is the main E/E system inside of HV battery to power electric or hybrid electric vehicles. The BMS consists of several input sensors (see Fig. 5) for cell voltages, cell temperatures, output current, output voltage, and actuators like HV contactors for disconnection. This system is connected to various powertrain control units, the charging interface (enabling the communication with battery charging stations), the on-board diagnostic interface, and via a dedicated gateway to the vehicle infotainment systems (including the human machine interface and a wireless internet connection).

For the demonstration of the applicability of the co-engineering framework we had to use existing tools, which have been extended for specific needs of the presented approach:

EPF-C[3] (Eclipse Process Framework – Composer) is used for tool-support regarding the safety and security process modelling (II).

WEFACT (Workflow Engine for Analysis, Certification and Test) [15], web-based distributed platform for requirements-based testing with continuous impact assessment in order to support the safety case with evidences. Test workflow was extended to a workflow for safety certification and in the EMC² project the attribute of security was integrated (III).

XSTAMPP (eXtensible STAMP Platform) [19] is an Eclipse RCP[4] based tool which guides users through the Safety and Security Co-analysis by STPA-Sec process and supports the modelling of control loops and the definition of constraints (VI).

OpenCert is an open source tool for product and process assurance/certification management to support the compliance assessment and certification of safety-critical systems in sectors such as aerospace, railway and automotive [14]. OpenCert supports creation of GSN structures and mapping of evidence to requirements demanded by underlying standards (V).

In the following, the main parts the framework in scope of the EMC² project will be described in more detail.

---

[2] Technology-specific details have been abstracted for commercial sensitivity and presented analysis results are not intended to be exhaustive.

[3] Eclipse Process Framework, www.eclipse.org/epf/.

[4] Rich Client Platform

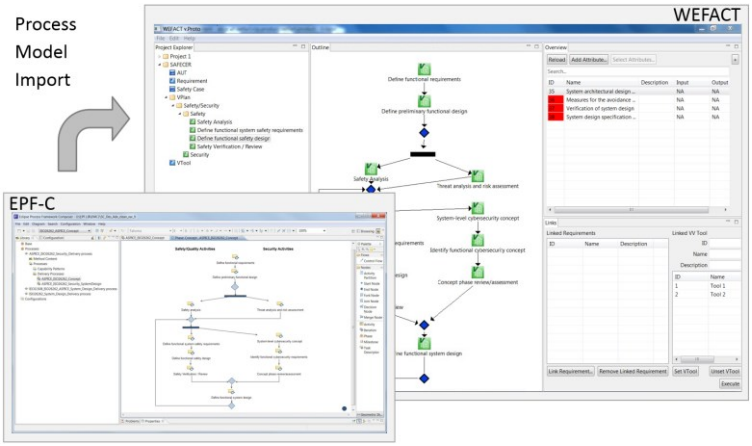

Fig. 4. Screenshots showing process modelling and execution (Tools: EPF-C, WEFACT)

4.1 Process Development and Process Execution

Efficient safety certification implies a process model which guides the user through the certification process and allows efficient compositional re-certification in the event of changes in the system. EPF-C provides elements to model phases and individual activities of the safety and security process. It allows modelling specific standards in a formal way, which enables automating the certification workflow.

WEFACT imports the process model including the activities modeled in EPF-C. Fig. 4 shows safety- and security-related parts of the assurance process. The modeled assurance activities (small squares in the model diagram) are imported as so-called V-Plans and displayed as hierarchical list in the project explorer (left part of the GUI window). The upper right section of the window shows the assurance ("V&V") activities contained in the selected V-Plan. The V-Plan can be associated with the respective assurance tools (lower right corner). Finally, the assurance activities are processed by the workflow engine and deliver evidences for the requirements. During workflow execution, the status of the assurance activities changes whenever an activity is completed; the altered status is indicated by different highlighted colors in the list of activities.

4.2 Safety and Security Co-Analysis using STPA-Sec

The main accidents related to the BMS are fire/explosion of the battery systems and collision with an object:

- Fire / explosion of the battery system could be caused on the one side by charging conditions which are due to manipulation or failures outside of the safe range, but also by a modification or error in the operating parameters.

- Similarly if the operating parameter of the battery system or the control module which provides power to the engines are modified or erroneous this could lead to undesired acceleration or deceleration which could cause a collision.

Fig. 5 shows the representation of the system architecture in the used XSTAMPP tool for the co-analysis. We focused on the control action "Charging Request" and identified the following unsafe control action, based on the guide phrase "Control Action given incorrectly": Excessive charging request is transmitted to charging unit during plug-in charging.

Potential safety and security scenarios for such an unsafe control action include:

- An excessive charging request can be caused by a modified charging request from the BMS to the charging unit due to tampered process model in the BMS software to enable fast charging for non-fast chargeable batteries. Potential motivation for the owner to hack his own car is that he is interested in faster charging and does not care about longevity of battery due to leasing contract for battery.
- A wrong charging request from BMS to charging unit may be caused by a failure/design error in the temperature sensor for a battery. Due to financial reasons a malicious manufacturer could reduce the number of sensors per battery cells below the number required for a reliable reading. One additional scenario is that a maintenance provider uses sensors with lower resolution and hacks the control system to accept these sensors which may be not certified for the task.
- Even when the vehicle BMS requests the correct power level a malicious manipulation on the communication between BMS and charging unit could lead to an unsafe charging request. Such a manipulation could be directed at the charging unit or the central charging management system at the backend.

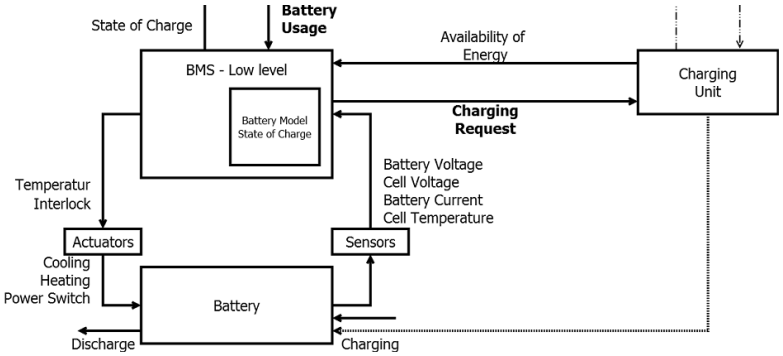

Fig. 5. Part of control loop of the battery management system (Tool: XSTAMPP) [20]

We use the tool XSTAMPP to identify potential safety-related accidents, based on potential causes from safety and security, e.g. failures and malicious manipulations by an attacker. In independent analysis the focus of security would be on the classical CIA properties (confidentiality, integrity and availability). The feedback of safety

relevance of certain properties is missing. Safety specific analysis focuses only on safety issues caused by faults of E/E systems. Scenarios in which a user modifies the vehicle and causes a potential safety hazard would be missed.

Co-Analysis connects the domains and supports the identification of safety goals and safety-related security goals.

4.3 Process- and Product- based Argumentation

Application of the methodology during the development of a BMS of a connected electrified hybrid powertrain starts with selection of underlying standards. In this use case we consider ISO 26262 and SAE J3061 which are modeled in EPF-Composer as standard compliant integrated process model. The intention is to consider interacting functional safety and security activities. Based on the process model we examine the concept phase which includes the Hazard Analysis and Risk Assessment (HARA). Results of the HARA are “Automotive Safety Integrity Levels” (ASIL), safety goals to mitigate potential safety-critical hazards and high level safety requirements. If security should be considered as well the necessary process steps based on SAE J3061 have to be added to the existing process model. In other words, the existing template based on ISO 26262 has to be extended with steps related to a co-engineering process. Executing this process means to perform co-analysis using STPA-Sec method. One result of the co-analysis is the hazard "overcharging battery during plug-in charging" for which developers have to implement an adequate countermeasure. Overcharging will be possible if an attacker modifies the BMU parameters. To document the relationship between requirements (represented as goals) and measures (declared in evidence documents) we use the OpenCert GSN editor. On the one hand the argumentation covers the safety and security process and on the other hand it deals with the product specific decision how to prevent "battery overcharge". From the security process point of view the top level claim is "define functional cybersecurity requirements to prevent unauthorized changes to BMU parameters". These requirements are listed in the corresponding project specific document "HV_Batt_SecReq" stored in the project repository. From the product side of view the BMU needs capabilities to detect and prevent unauthorized change of parameters. The documentation of these capabilities is evidence and usable as product-based argumentation.

4.4 Results of investigation

The presented co-engineering framework was demonstrated by application to a hybrid electric vehicle powertrain use case. The application of the methodology shows that the way how functional safety and security should correspond, has not been defined clearly up to now. The usage of patterns speeded up the process development activities and supported creation of argumentation fragments by GSN. GSN structures connect processes and evidence with argumentation. The graphical depiction of links between these elements improves the stakeholder’s understanding. The tool OpenCert provides the possibility to manage patterns and create GSN structures. In particular, this type of representation is an easy way to make clear how the dependencies be-

tween safety and security are organized. The execution of the assurance activities by the workflow engine WEFACT allowed widely automated generation of evidences for the combined safety and security case. The co-analysis method STPA-Sec was supported by the tool XSTAMPP.

5 Conclusion

Today's interconnected world needs special care to consider safety and security aspects. Although there are approaches treating the interaction between safety and security adequately they are still immature. This paper presented a safety and security co-engineering framework. A comprehensive combined safety and security argumentation methodology for the automotive domain has been developed. Its application in the automotive domain within the standards constraints provides useful information and can be considered as the next step for a wide application in development lifecycles. The following important benefits of the presented methodology for argumentation apply to the automotive domain: Usage of patterns speeds up the development e.g. process activities; the GSN structures connect process- and product-related evidence with argumentation; the graphical depiction of links between these elements improves the stakeholder's understanding of relevant safety and security aspects. In the HEV powertrain use case we showed the benefit of combined analysis of safety and security issues and the preparation of a security-aware safety case. GSN is an easy way to make clear how dependencies between safety and security are organized and why the selected trade-off is suitable.

The question, what is a compelling argument regarding a trade-off between functional safety and security which is able to pass the final assessment, has not been answered in a satisfactory manner and needs further investigation. The idea of safety and security co-engineering is becoming an accepted approach and it is required to appear in a specific standard regarding safety and security co-engineering activities and shall be treated in a normative manner. Experience gained in projects like EMC² will try to reach standardization committees and influence developments of future editions of standards with the goal of supporting assurance case establishment.

Acknowledgment

This work is supported by the projects EMC² and AMASS. Research leading to these results has received funding from the EU ARTEMIS Joint Undertaking under grant agreement n° 621429 (project EMC²), H2020-ECSEL grant agreement n° 692474 (project AMASS) and from the COMET K2 - Competence Centres for Excellent Technologies Programme of the Austrian Federal Ministry for Transport, Innovation and Technology (bmvit), the Austrian Federal Ministry of Science, Research and Economy (bmwfw), the Austrian Research Promotion Agency (FFG), the Province of Styria and the Styrian Business Promotion Agency (SFG).

References

1. Greenberg, A. (2015). Hackers remotely kill a jeep on the highway—With me in it. Wired, 7, 21.
2. Chen Yan, Wenyuan Xu, Jianhao Liu. (2016) Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle, DEFCON 24 conference
3. Borchert J., Slusser S. (2014, November). "Automotive (R)evolution: Defining a Security Paradigm in the Age of the Connected Car" Infineon Report Web http://www.infineon.com/car-security
4. Glas, B., Gebauer, C., Hänger, J., Heyl, A., Klarmann, J., Kriso, S., ... & Wörz, P. (2014). Automotive Safety and Security Integration Challenges. In Automotive-Safety & Security (pp. 13-28).
5. International Organization for Standardization. "ISO 26262 - Road vehicles – Functional safety, Part 1–10." ISO/TC 22/SC 32 - Electrical and electronic components and general system aspects, Nov. 15, 2011.
6. SAE: J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (2016)
7. Leveson, N. (2004). A new accident model for engineering safer systems. Safety science, 42(4), 237-270.
8. Macher, G., Sporer, H., Berlach, R., Armengaud, E., & Kreiner, C. (2015, March). SAHARA: a security-aware hazard and risk analysis method. In Design, Automation & Test in Europe Conference & Exhibition (DATE), 2015 (pp. 621-624). IEEE.
9. Schmittner, C., Gruber, T., Puschner, P., & Schoitsch, E. (2014). Security application of failure mode and effect analysis (FMEA). In International Conference on Computer Safety, Reliability, and Security (pp. 310-325). Springer International Publishing.
10. Goal Structuring Notation Working Group, GSN Community Standard Version 1, Nov. 16, 2011, www.goalstructuringnotation.info
11. Ray, A., & Cleaveland, R. (2015). Security Assurance Cases for Medical Cyber-Physical Systems. IEEE Design & Test, 32(5), 56-65.
12. Menon, C., Hawkins, R., & McDermid, J. (2009). Interim standard of best practice on SW in the context of DS 00-56 Issue 4. SSEI, University of York, Stand. of Best Practice (1).
13. Preschern, C., Kajtazovic, N., & Kreiner, C. (2013, October). Security analysis of safety patterns. In Proceedings of the 20th Conference on Pattern Languages of Programs (p. 12). The Hillside Group.
14. Ruiz, A., Larrucea, X., & Espinoza, H. (2015, September). A Tool Suite for Assurance Cases and Evidences: Avionics Experiences. In European Conference on Software Process Improvement (pp. 63-71). Springer International Publishing.
15. Kristen, E., & Althammer, E. (2015, September). FlexRay Robustness Testing Contributing to Automated Safety Certification. In International Conference on Computer Safety, Reliability, and Security (pp. 201-211). Springer International Publishing.
16. Macher, G., Armengaud, E., Kreiner, C., Brenner, E., Schmittner, C., Ma, Z.,… Krammer, M. (in press) Integration of Security in the Development Lifecycle of Dependable Automotive CPS. In Druml, N., Genser, A., Krieg, A., Menghin, M., & Hoeller, A. (Eds.), Handbook of Research on Solutions for Cyber-Physical Systems Ubiquity. IGI Global
17. Martin, H., Krammer, M., Bramberger, R., & Armengaud, E. Process-and Product-based Lines of Argument for Automotive Safety Cases., ACM/IEEE 7th International Conference on Cyber-Physical Systems. (2016)
18. Young, W., & Leveson, N. (2013). Systems thinking for safety and security. In Proceedings of the 29th Annual Computer Security Applications Conference (pp. 1-8). ACM.

19. Abdulkhaleq, A., & Wagner, S. (2015). XSTAMPP: an eXtensible STAMP platform as tool support for safety engineering.
20. Schmittner, C., Ma, Z., & Puschner, P. (2016, September). Limitation and Improvement of STPA-Sec for Safety and Security Co-analysis. In International Conference on Computer Safety, Reliability, and Security (pp. 195-209). Springer International Publishing.